

Metalogix[®] Archive Manager for Exchange 8.8

Hierarchical Storage Manager Guide



© 2023 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc. Attn: LEGAL Dept. 4 Polaris Way Aliso Viejo, CA 92656

Refer to our Web site (<u>https://www.quest.com</u>) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Metalogix are trademarks and registered trademarks of Quest Software Inc. and its affiliates. For a complete list of Quest marks, visit <u>https://www.quest.com/legal/trademark-information.aspx</u>. All other trademarks and registered trademarks are property of their respective owners.

Legend

- **CAUTION:** A caution icon indicates potential damage to hardware or loss of data if instructions are not followed.
- **IMPORTANT, NOTE, TIP, MOBILE OR VIDEO:** An information icon indicates supporting information.

Metalogix[®] Archive Manager for Exchange Updated August 2023 Version 8.8

Contents

Introduction	4
Installation	6
Configuration	11
Database	11
Stores	16
Optional Configuration	25
Advanced	25
Diagnostics	
Encryption	29
Packer	32
Tasks	34
Addendum	42
Remote HSM Server	42
HSM configured for Windows Server firewall	45
About Us	49
Contacting Quest	49
Technical Support Resources	49

Introduction

Hierarchical Storage Manager (HSM) as a data storage system, is a complement of several Metalogix archiving products. HSM can be installed in two ways:

- manually by the HSM installer
- automtically by the Metalogix Archive Manager installation package. When installed by the Installation package as a part of the Archive Manager product installation, necessary configuration is performed by the Installation package itself as described in the *Metalogix Archive Manager Quick Start Guide*.

This guide describes the manual HSM installation and configuration of HSM.

HSM allows storing of data (even all company data) on one or more file-servers. It is possible to use a shared store as well. HSM includes the Single Instance Store service (SIS), which ensures that identical content is stored only once. The SIS service activates version control, allowing the HSM system to keep track of any changes made to files or emails. With version control activated, the administrator may retrieve older versions. Even if the original file or email was deleted, it can be restored back.

The HSM Server (i.e. the computer where the HSM system is installed), as a complement of Archive Manager products, takes care of saving and securing archived documents. Archived data reside in store. HSM works with different store types depending on administrator's choice.

When archived with Archive Manager, the desired file or email with its attachments is transferred to the HSM system. It is the HSM System that takes care of storing and retrieving files/emails. The HSM system works with a database because the information contained in the shortcut is stored either in an ORACLE or MS SQL database. The HSM system passes down the file/email to a store specified by the administrator and this file/email is compressed *on the fly*. Only shortcut of a few kilobytes remains at the file/email's original location. This shortcut includes information about the new location of the archived file/email. The only difference a user notices is that the shortcut is displayed with a slightly modified icon.

Users may work with archived files/emails as usual which means: when an archived file/email is reopened, Archive Manager passes the information from the shortcut onto the HSM system. The HSM system restores the file/email from the store. For users it seems as if they are working in a normal environment.

The HSM system includes the Single Instance Store service (SIS), allows versioning in cooperation with Archive Manager products. Due to version control the HSM system keeps track of any changes made to a document, for example:

- who modified the document;
- when this modification occurred;

• what was modified within the document.

With version control activated, the administrator may retrieve older versions. Even files whose shortcuts were deleted can be retrieved as well.

Supported operating systems

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Software Requirements

- .Net Framework 4.5 if not available, Google Drive store will not be functional. If .NET Framework 4.5 is installed after HSM, it is necessary to run the HSM setup in "Repair" mode to activate the Google Drive store.
- IIS (32-bit support) if not available, setup will continue but the HSM web client will not be installed.
- Microsoft WSE 3.0 if not available, the iTernity store cannot be created.
- Database ORACLE Database (version 12c or higher), MS SQL Server (version 2014 or higher) or Azure SQL Database

Database requirements

- If you are using an MS SQL Database, then installation of MDAC (Microsoft Data Access Components) is necessary, as it contains the required OLEDB Data Provider for MS SQL Server. The MS SQL Data Provider for .Net is also needed for accessing MS SQL (part of the .NET Framework installation). We recommend installing the latest version of MDAC (Currently we recommend installing MDAC 2.8.)
- If you are using an ORACLE Database, and it has not been installed on the HSM server, then an ORACLE Database Client must be installed on your HSM server and a Net8 connection from the HSM server to the ORACLE Database server must be established. The ORACLE OLEDB Data Provider (part of the MDAC installation) and the Oracle Data Provider for .Net (part of the .NET Framework installation) are required for connecting the ORACLE Database. If you prefer working with an ORACLE Database, make sure to have similar data (database, database user, password, owner of the schema) available during the installation of Archive Manager for Exchange.

Databases with the database user(s) (who, in addition, should be the owner of the database) have to be available before HSM installation.

Installation

2

In this topic:

- Steps to download the install media
- Worksheet for this installation
- Steps to install HSM

Steps to download the install media

- 1. Login to the server with the credentials of the superuser (eg. democorp\mamadmin)
- 2. From your browser, navigate to the <u>https://www.quest.com/products/metalogix-archive-manager-for-exchange</u> page

or

navigate to the <u>http://www.quest.com/trials</u> page. Locate the product Metalogix Archive Manager for Exchange.

- 3. Click the **Download Free Trial** button.
- 4. Fill the *Download Your Free Trial* registration form and click **Download Trial**. The file download page appears.
- 5. Download the install media zip file.
- 6. The the trial license key is specified in the email that is sent to you.
- 7. Ensure that the files are available locally on the computer on which you are planning to install the Metalogix Archive Manager for Exchange features.

Worksheet for this installation

The following information will be required through the installation process. Sample values are provided here as a guidance.

ltem	Description	Example
HSM server	The server where the HSM and Archive Manager Search will be	AMXHSM

	installed.	
Superuser account	Windows account that is used to install the application and run the Archive Manager for Exchange services.	username: democorp\mamadmin password: *************
Media folder	Full path of the folder where the media files are extracted	C:\Metalogix
Installation folder	Full path of the folder where the application files will be installed	C:\Program Files (x86) \Metalogix
HSM Store folder	Full path of the folder that will contain the archived files.	C:\HSM The local hard drive folder is used as the default media store. Use of other media storage systems are described in the <i>Media Store Administration</i> <i>Guide</i> .
Store name	Name of the media store on a hard drive. With the <i>Advanced</i> <i>Installation</i> option of the installer wizard, only a local hard drive can be setup as a media store.	FILESTORE
Schema name	Name of a schema in a hard drive media store.	FILESCHEMA
Database Authentication method	Type of database authentication: Integrated Windows Authentication or SQL Authentication	Integrated Windows Authentication
UserLogin	Username if SQL Authentication is selected	dbadmin
Password	Database password if SQL Authentication is selected	*****
Database server	The database server instance name where the databases for	AMXDB

Archive Manager for Files will be	
installed.	

Steps to install the application

- Log in to the server (eg. AMXHSM) with the credentials of the superuser (eg. democorp\mamadmin)
- 2. Download the installation media. For more information see <u>Steps to download the install</u> <u>media</u>.
- 3. Run the Metalogix Archive Manager Installation Package to extract the files to a local folder.
- 4. Close the integrated installer wizard which starts automatically.
- 5. Run the HSM setup from <Media folder>\Archive Manager Installation Package\HSM**HSM Setup.exe**
- 6. A prerequisite check occurs and missing requirements if any are displayed. Click **Install** to ensure all missing requirements are installed.

HSM	×
	Welcome to the InstallShield Wizard for HSM
	The InstallShield Wizard will install HSM on your computer. To continue, click Next.
	< Back Next > Cancel

7. The *Welcome* window of the HSM installer opens.

8. Click Next. The Logon Information window opens.

HSM	×
Logon Information Specify a user account and password.	
Specify the user account to be used by this application. User accounts m DOMAIN\Username.	ust be in the format
Username:	
democorp \mamadmin	
Password:	
Confirm password:	
••••••	
InstallShield <u>Back Next</u> >	> Cancel

Enter the information as described below:

- a. Username logon name of the superuser (for example, democorp\mamadmin)
- b. Password logon password of the superuser
- c. **Confirm password** same as the Password.
- 9. Click **Next**. The *Firewall Settings* window opens.

HSM		×
Firewall Settings		
Allow programs to communicate throug	h Windows Firewall	
Instalishield	< <u>B</u> ack <u>N</u> ext >	Cancel

Select Allow programs to communicate through Windows Firewall.

10. Click Next. The *Ready to install the Program* window opens.

HSM			×
Ready to Install the Program The wizard is ready to begin installation.			
Click Install to begin the installation.			
If you want to review or change any of your inst exit the wizard.	tallation settin	gs, click Back. Clic	k Cancel to
InstallShield			
	< <u>B</u> ack	Install	Cancel

11. Click **Install**. The installation starts and the progress is displayed on the *Setup Status* window. When the installation completes, the *InstallShield Wizard Complete* window opens.

HSM	
	InstallShield Wizard Complete
	The InstallShield Wizard has successfully installed HSM. Click Finish to exit the wizard.
	< Back Finish Cancel

12. Click **Finish** to close the installer.

Configuration

In this chapter:

- Database
- <u>Stores</u>

Database

In this topic:

- Steps to configure the HSM database
- Steps to install the HSM database

Steps to configure the HSM database

- 1. When the installation completes, the *Configuration* wizard opens. If it does not open automatically, click **Start > Metalogix > Archive Manager Configuration**.
- 2. From the feature panel on the left, click **HSM** and select the **Database** tab.
- 3. Click Configure. The Database Connection Wizard opens.



4. Select either **Microsoft SQL Server** or **Oracle** and click **Next**. If you choose **Microsost SQL Server**, the *Database Connection* window opens for the Microsoft SQL Server connection information.

Database configuration		×
Database Connection Wiz	zard	2
Set up your Microsoft SQL S	Server connection.	
Please enter parameters which will	be used to create a connection to your Microsoft SQL Server	
Server name:	AMXDB	
Initial catalog:	MAMHSM	
Schema name:	dbo	
Authentication:	Windows Authentication 👻	
Username:		
Password:		
	< Back Next >	Cancel

For Microsoft SQL Server

- a. Server name name of the SQL server (eg. AMXDB)
- b. Initial catalog name of the HSM database (e.g. MAMHSM which is the default name of the HSM database)
- c. Schema name name of the SQL Schema (e.g. dbo)
- d. Authentication authentication type used for the database. Choose either Windows authentication or SQL Server authentication
- e. **Username** database login username if *SQL Server authentication* is the selected as the authentication mode.
- f. **Password** password of the database user if *SQL Server authentication* is the selected as the authentication mode.

For Oracle

- a. Oracle net name net service name that describes the network address of the database server in your tnsnames.ora file.
- b. Schema name of the Oracle schema from your tnsnames.ora file.
- c. Username database login username.
- d. Password password of the database user.
- 5. Click **Next** and then click **Yes** on the confirmation dialog that opens.

Database	configuration 🔀
$\mathbf{?}$	Database does not exists on the server. Shall we try to create it?
	Yes No

6. If the database connection is setup successfully, the configuration completion window opens.

Database configuration	×
Database Connection Wizard	S
You have successfully finished the Database Connection Wizard!	
Click on Finish to save your database connection parameters and update config files.	
If you have not done so already, you can execute the database scripts to create the necessary database objects.	
< Back Next > Fin	hish

7. Click Finish to close the Database Connection wizard.

Steps to install the HSM database

- 1. From the feature panel on the left in the *Configuration* tool, click **HSM** and then select the **Database** tab.
- 2. Verify that the database connection information is as expected. Then click **Run Scripts**. The script installer wizard opens.

Database configuration	×
Set up the database	
Specify the user under which to execute database scripts.	
Please specify user under which to execute database scripts. The user must be allowed to create or modify tables and procedures in the database.	
 Use the default credentials 	
O Use different credentials	
Authentication: Windows Authentication 👻	
Database user:	
Password:	
< Back Next > Cancel	

- 3. Select **Use the default credentials** to use the information displayed in the *Database connections* section. If you select **Use different credentials**, enter the following information:
 - a. Authentication authentication type used for the database. Choose either Windows authentication or SQL Server authentication
 - a. **Database user** database login username if *SQL Server authentication* is the selected as the authentication mode.

- b. **Password** password of the database user if *SQL Server authentication* is the selected as the authentication mode.
- 4. Click Next.



In the *Select the method for setting up the database* step, choose one of the following options:

- a. **Run the database scripts by this wizard** the installer will automatically run the scripts to create the tables and procedures required for the database.
- b. Get the database scripts and run them manually you get the option to either save the scripts or copy it to clipboard and paste it elsewhere.
- 5. Click **Next**. Depending on your selection, one of the following windows open:

For Run the database scripts by this wizard

Database configuration	×
Set up the database	
Select the database objects you want to create.	
Please select database scripts you want to execute.	
Create tables	
🕸 🔽 Create procedures	
< Back Next > Cancel	

Select both check boxes: Create tables and Create procedures.

For Get the database scripts and run them manually

Database configuration	8
Set up the database	
Get the database scripts	you want to execute manually.
Get the selected scripts and execute the	m manually in an external application.
Tables	Procedures
Save the script	Save the script
Copy to clipboard	Copy to dipboard
	< Back Next > Cancel

You must run both the scripts for a successful database installation.

- 6. Click Next. Depending on your selection in step 4, one of the following windows open
 - a. If you chose **Run the database scripts by this wizard**, and the installation is successful, a confirmation dialog opens. Click **OK** to close the dialog.
 - b. If you chose **Get the database scripts and run them manually**, you must run the scripts immediately because a confirmation dialog will verify whether you ran the scripts.

Confirm		×
?	Please confirm that you have successfully executed the following database scripts:	
	☑ Tables	
	✓ Procedures	
	OK Cancel	

Select both check boxes after you run scripts and click **OK**.

7. If the installation is successful, the confirmation dialog opens. Click **OK** to close the dialog. The database setup completion window opens.

Database configuration	×
Set up the database	
Database setup wizard has finished.	
The database scripts were executed successfully.	
< Back Finish Cancel	

8. Click **Finish** to close the script installer. The *Scripts* section of the *Configuration* tool displays the status and version of the scripts(the version of the scripts you install may differ from the version shown in the image below).

🞇 Configuration					
Configure HSM	Datab	ase Stores	Advanced	Diagnostics	Encryption Packer Tasks
🕡 н5м 🕨	Database conne Provider: Server name: Initial catalog: Schema name: Username:	Microsoft SQI AMXDB MAMHSM dbo (Windows Au	L Server)	
	Scripts				Configure
	Database version: Scripts version:	X.X.0.XX X.X.0.XX			
SS	🥝 Your database i	s up to date.			Run scripts

9. Keep the *Configuration* tool open for next steps.

Stores

In this topic:

- <u>Steps to configure a media store</u>
- <u>Steps to configure a schema</u>
- Steps to test the HSM and Media Store connectivity

Steps to configure a media store

- **NOTE:** A large selection of supported media store types are described in the *Media Store Guide*.
- 1. From the feature panel on the left of the *Configuration* wizard, click **HSM** and select the **Stores** tab.
- 2. From the *Stores* section click **New Store**. The *Create a new media Store* window opens.

Media Store Administration Wizar	d	×
Create a new Media Stor	e	
Choose a na	ame and type for the Media Store.	
Media Store type:	Jukebox, Harddisk, Network Share 🔹	
Name of the new Media Store:	FILESTORE	
	< Back Next > Cancel	

3. Click Next. The location information window opens.

Media Store Administration Wizard		
Jukebox, Harddisk, N	etwork Share	
Choose Use a su	a location where the archived files should be saved. pported storage provider for this Media Store.	
Storage provider :	Hard disk, UNC Path	
Path for the Media Store:	C:\HSM	Browse
Allow multiple saving:		
Path for multiple saving:		Browse
Path for fast file access:		
Retention time support:	<none></none>	
	< Back Next >	Cancel

Enter the information as described below;

- a. **Storage Provider** select Hardisk, UNC Path because we are going to setup a media store in folder on the local hard drive.
- b. **Path for the media store** browse and create the folder if it does not exist (eg. **C:\HSM**). You could specify a UNC path to a shared folder as well.
- c. Allow multiple saving select this check box if you want to archive the file in an alternate location. For example C:\HSM-Backup.
- d. **Path for multiple saving** alternate media store location. Browse and create the folder if it does not exist (eg. **C:\HSM**). You could specify a UNC path to a shared folder as well. This field is available if **Allow multiple saving** selected.
- e. Path for fast file access choose between the Path for the media store and Path for multiple saving that are listed in the drop-down. Typically, if the first path is a slow media store like Pegasus Jukebox, and the second path is a large SAN like a local RAID or Harddisk, then you should use SAN because it is much faster. This field is available if Allow multiple saving selected.

NOTE: If archiving to one path fails, file store operation will result in an error.

- f. **Retention time support** from the drop-down box, select one of two predefined retention time support options:
 - NetApp SnapLock if you are using NetApp and want to use SnapLock for compliance with law regulations about archiving of electronic documents. (e.g. HIPAA, OFRS, COSO etc.)
 - EMC Celerra if you use EMC Celerra.
- 4. Keep clicking **Next** to accept the default settings on each window until you reach the HSM server connection information window. Every media store must provide this information so the HSM server can connect to it. For more information about various media stores see the *Archive Manager for Exchange Media Store Administration Guide*.

Media Store Administration Wizard	×
Jukebox, Harddisk, Network Sha	are
Please choose the PamS Please choose how long the PamServers. This giv before the Media Store the HSM Servers where the Media Store sh AMXHSM(H	Servers where the Media Store should connect to: g the Media Stores pauses before it tries to connect to ives the PamServer the possibility to start completly e tries to connect to this PamServer the first time. hould connect to:
	Add Server
🛨 Add	• Specify the server where this store should connect.
Connection interval between the Media	a Server type: HSM Server 🔹
	Server name: AMXHSM
	OK Cancel

- 5. Click Add. The Add Server window opens. Enter the following information:
 - a. Server type select HSM Server
 - b. Server name name of the server where HSM is installed (eg. AMXHSM)
- 6. Click **OK** to close the window and add the the HSM Server to the list.
- 7. Click **Next**. The final configuration window appears.

Media Store Admi	nistration Wizard	×
Jukebox, Ha	rddisk, Network Share	
	The wizard has finished collecting the information needed to create the Media Store.	
	Relative speed of the store:	
	Use HSM Cache for read operations:	
	Write protection (mark as read-only):	
	Re-create service for this Media Store:	
	< Back Finish Cancel	

8. Accept the defaults and click **Finish**. The *Service Restart* window opens.

Restart service	
Service restart needed	÷.
To apply the changes you have made, t restarted:	he following services should be
Name	Status
MAM HSM Base Operations MAM HSM Asynchronous Operations	Running Stopped
Do you want to restart the selected ser	vices?
	Yes No

Select one or more check boxes where the **Status** indicates **Stopped**. Click **Yes** to restart the service so that the HSM service is aware of the media store configuration.

9. Verify that the media store information appears in the *Stores* tab of the *Configuration* wizard.

🞇 Configuration	
Configure HSM	Database Stores Advanced Diagnostics Encryption Packer Tasks
🕡 нsм 🕨 🕨	Id Name Server Mirror of State 1 FILESTORE AMXHSM Running
	New store Set up Delete Primary Manage Refresh Schemas Id Name Store Server Force Store Encryption Key Compression Task
SS	🕂 Create 🔀 Edit 🔀 Delete 💟 Test 🔁 Refresh

Steps to configure a schema

1. From the *Schemas* section in the *Stores* tab of the the *Configuration* wizard, click **New Schema**. The *Create new schema* window opens.

HSM Schema	8
Create new	r schema 🛛 😥
Store: Schema name:	FILESTORE@AMXHSM FILESCHEMA
Allow duplicate:	
Encryption:	<none></none>
Task:	<none> •</none>
Compression:	
Exclude files:	.gz;.zip;.rar;.jpg
	Use ";" as separator and include the "." in extensions. Example: .zip;.jpg;.rar
Packer:	<none></none>
	OK Cancel

- 2. Enter the following information:
 - a. **Store field** select a media store from the drop-down list that must be linked to this schema.
 - b. Schema name enter a name for the schema (eg. FILESCHEMA)
 - c. Allow duplicate select the check box to activate duplicate archiving. For example, when you archive a file in in Store A (linked to schema 1) and then archive it again in store B (linked to schema 2), the file is recognized as a duplicate and is archived to both stores.
 - d. Encryption choose the appropriate encryption from the drop down list
 - Task select a task from drop-down list that you want to assign to the schema. The task will run when the file is archived with the schema, e.g. copying the file to another media store. You must first create a task in the <u>Tasks</u> tab, but tasks with a delete operation are not displayed in the drop-down list.
 - f. Compression select this check box to compress files as they are archived.
 - g. Exclude files file types that you do not want to compress are listed here. This field is activated only if Compression is selected. List the desired files extensions by using a semicolon (;) to separate each extensions and prefix each file extension with a dot (.).
 - h. Packer select a packer from the drop-down list. Packers join multiple files stored in HSM into large ZIP archives. Several large files as opposed to small ones increases disk space utilization and avoids internal disk fragmentation. Packers must be created in the Packer tab. It is not possible to have packer and task selected at once. If you must use a packer together with some other task operations, a packer operation can be defined directly as a task operation.
- 3. Click **OK** to save the schema information. In the *Service Restart* window that opens, select one or more check boxes where the **Status** indicates **Stopped**. Click **Yes** to restart the service so that the HSM service is aware of the schema information.

4. Verify that the schema information appears in the *Schemas* section of the *Stores* tab in the *Configuration* wizard.

🎇 Configuration	- 6 🛛
Configure HSM	Database Stores Advanced Diagnostics Encryption Packer Tasks
🕡 нรм 🕨	Stores Id Name Server Mirror of State 1 FILESTORE AMXHSM Running
	New store Set up Delete Primary Manage Refresh Schemas
	Id Name Store Server Force Store Encryption Key Compression Task 1 FILESCHEMA FILESTORE AMXHSM
SS .	🕂 Create 🔀 Edit 🔀 Delete 🗹 Test 🔁 Refresh

5. Close the *Configuration* wizard.

Steps to test the media store connectivity

- 1. Open the *Configuration* wizard and select HSM from the feature panel.
- 2. Click the **Stores** tab. Then click **Test** from the **Schemas** section. The *HSM Test* window opens.

HSM Server:	AMFHSM.der	ocorp.com	
File identifier:			
Identifier type:	G HsmId	C Guid	<u>Name to FileId</u>
	📃 Archive	📑 Retrieve 🕞 🗙 Delete 🕱 Set r	etention 🛛 🔅 Mass actions 🔹

3. Click Archive. The Archive window opens.

Archive	8
Target schema:	FILESCHEMA (FILESTORE)
Retention time:	Fixed value O months
	C Infinite
	C Indefinite
• Use generated test files	
Unique content:	2020092723000026728376dbdad49508b431b80d988b473f0254d
Original filename:	TestFile.txt
O Use a specific test file	
Path to test file:	
Options:	✓ Make each file unique
	Use invalid checksum Do not compress
	Archive empty file
	Archive Close

Enter the following information as necessary:

- a. Target Schema select the schema and media store pair from the drop-down list.
 - **Retention time** select from one of three retention time options to test how long an archived file will be retained in the media store:
 - Fixed value file will be retained for the number of months specified in the field.
 - Infinite file will be stored for ever.
 - Indefinite no specific retention time but it can be defined later.
- b. Use generated test files select this option if you want the system to generate a test file.
 - Unique content click 🖄 to let the system generate a unique content for the systemgenerated test file. Copy the value in the Unique content field if you wish to test the retrieve process.
 - Original filename name of the file that will be tested. You can keep the default file name or specify a different file name.
- c. Use a specific test file select this option if you want to use you own file to test. Enter the full file path in the Path to test file field or click to browse for the file.
- d. **Options** select one or more of the following to test additional archiving features.
 - Make each file unique new unique string is generated after each test archiving
 - Use invalid checksum select to test checksum verification.
 - Archive empty file select to test empty file archiving.
 - Compress select to compress test files.
 - **Do not compress** select for no compression even if the compression is activated.

- Activate logging select to log the test operation.
- 4. Click Archive. The *Result* window opens.

Resul	t		×
~	Step 1:	Success	
•	HsmId:	1	
	Guid:	n/a	
~	Step 2:	Success	
	HsmId:	2	
	Guid:	n/a	
Elap	sed time:	00:00:00.2023647	
File	size:	32.0 KB (32768 bytes)	
			ОК

- 5. Verify that the result indicates success. Then click **OK** to close the *Result* window. Then close the *Archive* window.
- 6. In the *HSM Test* window, enter the name of the file that was archived in the Media Store during the archive test.

ł	ISM Test		×
	HSM Server:	AMFHSM.democorp.com	
	File identifier:	0000001	
	Identifier type:		
		📮 Archive 🔄 Retrieve 👻 Delete 🔣 Set retention 🛛 🐯 Mass actions	•
		Close	

For example if the TestFile.txt was archived as 00000001.txt, enter **00000001** in the **File Identifier** field.

7. Click **Retrieve**. The *Result* window opens.

\checkmark	Result:	Success
	Id:	1
	Name:	TestFile.txt
	Size:	32.0 KB (32768 bytes)
	Elapsed time:	00:00:00.0476363

8. Verify that the result indicates success. Then click **OK** to close the *Result* window. Then close the other windows.

4

Configuration options described in this chapter are optional. They provide administrator with diagnostic, encryption, compression and async task possibilities.

In this chapter:

- Advanced
- **Diagnostics**
- Encryption
- Packer
- <u>Tasks</u>

Advanced

This tab is used to configure the more advanced settings of HSM as single instancing, cache settings and temporary folder. After configuring all options press the **Apply** button.

🞇 Configuration					X
Configure HSM	Database	Stores Advanced	Diagnostics	Encryption Packer Task	s
KIM K	Duplicate files detect Duplicate detection metho © Detect by content © Detect by checksur © Do not detect dupl © caching Cache directory: Minimum cache size: Clear the cache ©	tion) d to be used: n icate files 409 <u>-</u> MB 512 <u>-</u> MB		Browse	
55	Temp directory:	%TEMP%		Browse	

Duplicate files detection

Since the HSM system includes the Duplicate Files Detection service, it means that identical files are stored only once. In the **Duplicate files detection** section you may specify the detection method:

- 1. Select the **Detect by content** option, should you wish to use the size, checksum and content for detection.
- 2. Select the **Detect by checksum** option, should you wish to use the size and checksum for detection;
- 3. Select Do not detect duplicate files option, should you wish to deactivate this detection

If Allow duplicate in the Advanced tab is checked, the file is stored in both stores.

Caching

Use caching in case of slow storages (tape etc.). HSM will cache the recently used files to speed up the retrieving process.

If **Activate caching** is checked, HSM will copy all retrieved files to an HSM internal cache. To set the **Cache directory** (which should be a local hard disk), use the **Browse** button next to the respective text box. If you have a cluster, the HSM will know that each installation has its own path.

Set the **Minimum cache size** and **Maximum cache size** as well. The **Minimum size** should be about 80% of the cache size. If the cache is full, HSM will delete files (the oldest first) until the cache reaches the "minimum size".

NOTE: To choose which Media Store should be cached, use the MediaStoreAdministrator tool. It is started when you click Launch on the Stores & Schemas tab.

Temporary

The HSM stores temporary files created during duplication detection, compression etc. in temporary directory. Its location can be set in **Temp directory** text box. Usage of environment variables is allowed in this box (e.g. %TEMP% denotes the temp folder of the currently logged on user).

Diagnostics

From time to time administrators need to check systems they manage, examine and analyze their behavior. This tab provides access to features that facilitate this task. Logs and tracing record HSM actions specified by the administrator at the defined extent.



Manage trace settings

In the HSM Trace Settings configuration you can activate various kinds of loggings for the specific HSM components. Select the component in the list and then configure it by checking/unchecking the desired check boxes. Multi-select is possible.

HSM Trace set	tings				×
Trace set	tings				
Component PamHSM PamHSMDB PamHSMAsync PamHSMCrypt PamServUtil PamServUtil PamStream PomaAmass POMAPeg	Debug St	Log performance	Performance entry	Redirect debug	Redirect file
🗌 Debug outp	ut		Redirect outp	ut to trace file	
Performance	e logging		Redirect outp	ut to debug outpo	ut
Peformance	logging (w	vith entry)			
Trace file:	Open file	Clear file Ac	ld comment		Browse
				ОК	Cancel

You can activate verbose logging (**Debug Output**), two kinds of performance loggings (logging information after a specific operation is completed or before a specific operation begins – **Performance logging** and **Performance logging (with entry)** and choose whether you want to redirect outputs either to debug output (**Redirect output to debug output**) or to the given trace file (**Redirect output to trace file**). In the case of **Redirect output to trace file** the path has to be specified in the **Trace File box**. The trace information will be logged there. You can also Open the

trace file with the **Open file** button or delete its contents with the **Clear File** button. If you clear the file then the file itself won't be deleted. Use **Add comment** in case you wish to add some text to the file.

After changing the settings you want click the **OK** button. If you want to discard them click the **Cancel** button.

Manage log settings

In the Log settings dialog configure the overall HSM logs to your needs:

Include message levels - define which information should be logged

- \circ Errors only
- Errors and warnings
- Errors, warnings and Information

Debug output - check to activate verbose logging

Log file – check to save the messages in log files

Path - set logs location

Name prefix – define naming convention; log file name will include this prefix and a number

Number of files – if a new log file should be created when the limit is reached, the oldest log file will be deleted

Size of each file – when the defined size is reached, new log file will be started

Click **Open the current log file** to open it.

Clicking the **Clear all files** will delete all logs.

Log settings			X
Log sett	ings		
C Log level			_
_80	Include message level	s:	
	Errors, warnings and i	nformation 🔻	
C Log targe	et		2
6	Debug output		
	🖌 Log file		
	Path:	Program Files (x86) \Common Files \PAM \HSM \Log Browse	
	Name prefix:	PamLog	
	Number of files:	17 .	
	Size of each file:	512 • kilobytes	
		Open the current log file	
		<u>Clear all files</u>	
			_
		OK Cancel	

Encryption

The Encryption tab allows you to manage encryption keys that are used to safeguard your archived items stored in HSM.

🛠 Configuration	
Configure HSM	Database Stores Advanced Diagnostics Encryption Packer Tasks
🕡 HSM 🕨 🕨	Id Name Type Key from different server
	😋 Export 💽 Import 📑 Create 🖉 Modify 🔀 Delete
0	WARNING: If the key is lost, all files encrypted with it will be unreadable. Be sure to export the key and store it in a safe location.
52	

Steps to create an encryption key

1. In the *Encryption* tab, click **Create**. The *Create new encryption key* window opens.

HSM Encryption	×
Create new encryption key	R
Key name: Primary Key	
Key Type: 🔿 RC4 💿 AES256	
ок	ancel

Enter the information as described below:

Key name - display name of the encryption key.

Key type - Select one of the industry standard encryption ciphers **RC4** or **AES256**. Between the two, AES256 is a relatively new and very complex 256-bit block cipher, and RC4 is a very old and simple stream cipher.

2. Click **OK** to create the encryption key. The *Configuration* window opens.

Configurat	Configuration			
$\mathbf{?}$	The key was successfully saved to the database. It is highly recommended to export the key. Do you want to export it now?			
	Yes No			

- 3. Click **Yes** to export the key or click **No** to export it later. If you click **Yes**, the *Export Encryption Key* window opens. See the section below for steps to export the encryption key.
- **NOTE:** Always export and store encryption keys in a safe location. If the key is lost, it will not be possible to read the encrypted files.

Steps to export an encryption key

- 1. There are two ways to export an encryption key:
 - a. Select an encryption key from the encryption key list and click **Export**.
 - b. Create a new encryption key and click **Yes** in the *Configuration* window that opens after you have created the key.
- 2. In the Export Encryption Key window, enter the information as described below.

HSM Encryption				×
Export Encryption K	ey			R
Path to keyfile:				Browse
Password for encryption:				
Confirm password:				
		1	Export	Cancel

- a. Path to key/file location where the key will be exported. Click Browse to open the Save As window. The default location is C:\Program Files (x86)\Common Files\PAM\HSM\Keys. Keep the default or choose a location. Then enter a name for the encryption key file and click Save.
- b. Password for encryption enter a password for the encryption file.
- c. Confirm password enter the password again to confirm the password entry.
- 3. Click **Export** to export the encryption key.

Steps to import an encryption key

1. In the *Encryption* tab, click **Import**. The *Import Encryption Key* window opens.

HSM Encryption		×
Import Encryption Key		R
Path to keyfile:		<u>Browse</u>
Key name:		
	Import	Cancel

- 2. Enter the information as described below:
 - a. Path to key/file location from where the key will be imported. Click Browse to select a location.
 - b. Password for encryption enter a password for the encryption file.
 - c. Key name name of the encryption key file.
- 3. Click Import to add the encryption key to the HSM encryption key list.

Steps to modify an encryption key

1. Select an encryption key from the encryption key list and click **Modify**. The Edit Encryption Key window opens.



- 2. You can change the *Key name* of the encryption key but you cannot change the *Key Type*.
- 3. Click **OK** to save the change.

Steps to delete an encryption key

- 1. Select an encryption key from the encryption key list
- 2. Click Delete. A confirmation window opens.
- 3. Click **Yes** to confirm the deletion of the encryption key.

Packer

Packers are joining multiple files stored in HSM into large ZIP archives. It is better to have several large files than a plenty of small ones – the disk space utilization is more efficient in this case, because it helps to avoid internal disk fragmentation. Packers can be created and managed on the **Packer** tab. Created packers can then be assigned to specific schema on the **Stores** tab.



First select the store in **Temporary store for packages** dropdown. It will be the temporary store for archived files before they got packed. Then the packed files will be moved to the final store (it can be the same store as well).

To create a packer, click **Create**. The HSM Packer dialog pops-up. Configure the settings:

Name	– enter packer name
Туре	– the file to be used by the packer
Max. package size	 if the specified limit is reached, new package will be created
Max. files in package -	package starts to be created when the specified number of files is reached
Max single file size	 if the file size is bigger than the specified value, the file will not be included in the package (otherwise it would be much time consuming)
File types & Action package	– allow specifying file types to be included / excluded in/from the

Max age of files — is files to be packed are waiting in the packer queue longer than the specified value, a new package will be created

Deactivate processing of files – deactivate processing of files in the packer queue

HSM Packer	×
Create HSM Packe	r
Name:	
Туре:	zip 🔹
Max, package size;	100 🕂 MB
Max. files in package:	1000
Max, single file size:	100 🕂 MB
File types:	.zip;.rar
	Action: exclude 🔹
Maximum age of files:	43200 🗧 seconds
Deactivate file processing:	
	OK Cancel

Following table displays how archived files in HSM are handled during 'Asynchronous packer' task process:

Temporary store for packages	Source Store result	Target store result
Same as Source store (*)	Original archived files are deleted after they are compressed and stored in Temporary store for packages.	ZIP container with archived files
Different as Source store (*)	Original archived file remains at store after they are compressed and stored in Temporary store for packages.	ZIP container with archived files

Temporary store for packages: HSM store that is used by packer process to store compressed temporary files that are subsequently stored in ZIP container. Current version of HSM uses only GZ compression.

Source store: HSM store that is processed by 'Asynchronous packer' task.

Target store: HSM store where ZIP containers are stored as a result of 'Asynchronous packer' task

NOTE: Files archived into HSM with compress option activated at schema always remains at source store regardless settings of temporary store for packages. These files also do not use 'Temporary store for packages' since they are already compressed. This behavior is by HSM design.

Tasks

On this tab you can create asynchronous tasks for HSM. An *asynchronous* task can be performed at a later time and not immediately after its creation. Basic tasks are the following:

- Copy copies archived items from a source store to a destination store.
- Move moves archived items from a source store to a destination store.
- Encrypt encrypts files in the specified store with a selected encryption key.
- Advanced define multiple tasks or sequence tasks based on specific criteria.



Creating Move / Copy task

- **NOTE:** Before creating any asynchronous task, stores must be created under the **Stores** tab.
- 1. Click Create > Move task (or Copy task). The Move files (or Copy files) window opens.

New task		×
Move files		
Create task movi	ng all files from the selected store to another.	
Source store:	FILESSTORE@40ADDC1	
Target store:	NEW STORE@40ADDC1	
Name:		Generate
Description:		
Resume at FILEID:	0	
Active:		
Auto-deactivate:		
Scheduling:	Id Start Stop 0 anytime never 1 10:38 AM 10:38 AM	
	🛨 Define 🛛 🖉 Modify 🚽 🔀 Delete	
	ОК	Cancel

Enter the configuration details as described below:

- a. Source store dropdown menu select the store from which the files will be moved (copied).
- b. Target store dropdown menu select the store to which the files will be moved (copied).
- c. **Name** text box type the task display name or click *Generate* to fill in the text box with generic name.
- d. **Description** add a description about the task.
- e. **Resume at FILEID** select the check box if you want the task to "remember" the last processed file and resume at the next one when it starts again after a pause. (The textbox displays the file ID of the latest processed file.)
- f. Activate select the check box to activate the task.
- g. **Auto-deactivate** select the check box to deactivate the task when it completes. The check box is available only when **Resume at FILEID** is checked.
- h. **Scheduling** Sets the task run time. Besides the default perpetual unlimited scheduling, you can add your own start time and stop time by clicking **Define**. There can be several schedulers defined. Then select the actual scheduling time. The task will be started every day at the defined time.
 - **NOTE:** Task scheduling can be modified when you select the task from the list and click **Modify**. If *anytime* is selected the task starts whenever the MAM HSM Asynchronous Operations service starts.
- 2. Once the task is configured, click **OK**. The task displays in the *Tasks* list.

Creating Encryption Task

- **NOTE:** Before creating any asynchronous task, stores must be created under the Stores tab.
- 1. Click **Create** > **Encrypt task**. In the *Encryption Task* window opens.

New task		×
Encryption Task		
Encrypt store wi	th given encryption key	
Source store:	•	
Encryption Key:	-	
Name:		Generate
Description:		
Resume at FILEID:		
Active:		
Auto-deactivate:		
Scheduling:	Id Start Stop	
	0 anytime never	
	🚹 Define 🛛 Modify 🔀 Delete	
	ОК	Cancel

Enter the configuration details as described below:

- a. Source store dropdown menu select the store to which the files will be encrypted
- b. **Name** text box type the task display name or click Generate to fill in the text box with generic name.
- c. **Description** It is a good practice to add a short Description of the task.
- d. **Resume at FILEID** Select the check box if you want the task to *remember* the last processed file and resume at the next one when it starts again after a pause. (The text box displays the file ID of the latest processed file.)
- e. Activate Select the check box to activate the task.
- f. **Auto-deactivate** Select the check box if you wish to deactivate the task as soon as it completes. The check box is available only when **Resume at FILEID** is checked.
- g. **Scheduling** specify the task run time. Besides the default perpetual unlimited scheduling, you can add your own start time and stop time by clicking **Define**. There can be several schedulers defined. Then select the actual scheduling time. The task will be started every day at the defined time.
 - **NOTE:** Task scheduling can be modified when you select the task from the list and click **Modify.** If *anytime* is selected the task starts whenever the MAM HSM Asynchronous Operations service starts.
- 2. Once the task is configured, click **OK**. The task displays in the *Tasks* list.

Creating Advanced Task

Advanced task allow configuration of specific task criteria. To create the Advanced task:

1. Click Create / Advanced option from the menu. Task wizard opens.

Task			×			
Async	hronous task					
~	Enter the general properties for the asynchronous task.					
	Store:	FILESSTORE@40ADDC1 •				
	Task name:	Custom task				
	Description:					
		< Back Next >	Cancel			

In the first dialog enter the general task configuration:

- a. Store select the source store for which the task should apply
- b. Task name enter tasks display name
- c. Description it's a good practice to add short task description
- d. Click Next.
- 2. Advanced task can consist of several operations. This dialog allows you to define the operations and the sequence in which they should be performed. To do so, select the operation in the **Operations** list and click the arrow to add the operation to the **Task operations** list. The operation sequence can be customized easily by selecting the desired operation and moving it up or down by clicking the **Move up / Move down** arrows under the list.



- 3. In case no operation is created in the **Operations** list or you wish to create a new one, click the **Create** button. You will be able to create:
 - a. Store operation (Copy, Move and Delete) or
 - b. Packer operation
 - c. Encrypt operation

Task					×
Asynchronous task					
Define store operations and build the se asynchronous task.	quence of o	operation	is to be	peformed by the	
Operations:			Task op	perations:	
Id Name	Туре		Id	Name	
1 Encrypt STORE with encryption key: AES256	Encrypt				
Store operation					
Packer operation					
Encrypt operation	>		<	III	>
🛨 Create 🕞 🕢 Modify 🛛 🔀 Delete			🚹 Mo	ve Up 🔣 Move Dowr	1
			Back	Nexts	Cancel
			Dack		Cancer

Store operation

a. In case the **Create/Store operation** has been selected, the Store operation configuration dialog opens. The source store will be the store you have selected in the previous dialog. In the dialog enter the operation configuration:

Task			×
Store opera	tion		
Source store:	FILESSTORE@40ADDC1		
Operator:	Сору	•	
Target store:		•	
Name:			<u>Generate</u>
	OK		Cancel

- i. **Operator** select the type of store operation you wish to create (Copy, Delete, Move)
- ii. Target store target store where ZIP archives are stored
- iii. **Name** Name of the operation. To generate the name automatically click **Generate** button.
- b. To confirm, click **OK**.

Packer operation

a. In case the **Create/Packer operation** has been selected, the Packer operation configuration dialog opens. In the dialog enter the operation configuration:

Task				×
Packer oper	ation			
Packer:	test (1)		•	
Target store:			•	
Name:				<u>Generate</u>
		OK		Cancel

- i. **Packer** select the packer which the task should apply. Packers are defined in **Packer** tab.
- ii. Target store target store where ZIP archives are stored.
- iii. **Name** Name of the operation. To generate the name automatically click **Generate** button.
- b. To confirm, click OK.

Encrypt operation

a. In case the Create/Encrypt operation has been selected, the Encrypt operation configuration dialog opens.

Task		×
Encrypt oper	ation	
Source store:	STORE@WIN2012R2]
Encryption key:	AES256(AES256)]
Name:		<u>Generate</u>
	OK	Cancel

- i. Source store will be the store you have selected in the previous dialog.
- ii. **Encryption key** select the encrypt which the task should apply. Encryption key is defined in Encryption tab.
- iii. **Name** Name of the operation. To generate the name automatically click **Generate** button.
- d. To confirm, click **OK**.
- 4. Click **Next**. Set up filters defining files to be processed from the source store. To do so, click the filter you want to use from the left pane:
 - a. Resume at the task will start from the specified file
 - b. Schema specifies the schema under which the files are store
 - c. Expired (yes/no) specifies whether files where retention time has expired should be processed
 - d. File ID specifies the ID of files

- e. Date specifies the archive date
- f. Size specifies the file size
- 5. The filter displays in the main pane where you can configure it. To remove the selected filter, click its name again.

Task			Đ
Asynchronous task			
? Set up the criteria fo	r files to be process	ed by this asynchronous task. Query Builder SQL View	
Filters	Store:	FILESSTORE@40ADDC1	
Resume at Schema	File size:	not specified	
Expired	Schema:	schemaOne 👻	
Date	Creation date:	not specified • 8/20/2017 • not specified 2/20/2018 •	
Size		equals before after between	
		< Back Next > Cancel	_

SQI View tab – displays the defined filter criteria in SQL View. When you are modifying already existing task it is not possible to edit the query using the Query Builder directly. You have to edit your query in the SQL view. Should you want to use the Query Builder, you have to create a completely new query.

- 6. Click **Next**. Set the task scheduling. Make sure to check the **Active** check box to activate the task.
 - a. To set **Run interval** when the task will be performed, select the desired option from the list or click **Define** button to set up custom interval.
 - b. Check **Auto-deactivate** should you wish the task to become inactive as soon as it carries its work out. The check box is available only when **Resume at FILEID** filter is defined.
- 7. Click Finish.

Once the task is created, it displays in the Asynchronous task list view. Menu under the Asynchronous Tasks list provides access to the following functions:

- Create create a new asynchronous task; two most common tasks can be created directly:
 - \circ Move task
 - \circ Copy task
 - \circ Encrypt task
- Advanced specific tasks can be created via wizard that is launched.
- Change change settings of the task selected in the list view (for detailed description see the section "Creating Advanced Task")
- Delete task delete the selected asynchronous task

- Action access to immediate Start, Stop or Restart of the selected task
- Logs view log of the selected task or clear the respective log or logs of all tasks
- **Refresh** refresh the tasks list

Addendum

In this chapter:

- <u>Remote HSM Server</u>
- HSM configured for Windows Server firewall

Remote HSM Server

In case of a remote HSM Server, i.e. if the HSM Server is installed on a separate machine, it is necessary that:

- a) the *HSM Base service* runs under the Archive Manager super-user account
- b) DCOM Rights are reduced
- a) The Archive Manager super-user account is an account under which our MAM services (MAMfsaHandlerSv, MAMfsaRemoteSV, MAMfsaArchiverSv) run on the Archvie Manager server.

On the HSM server, follow these steps:

- **1.** Open Start / Administrative tools / Services and locate the *MAM HSM* Base Operations service.
- 2. Right-click it and open its Properties. On the Log On tab check This account option and enter the super-user account with its password. (Super-user account is an account which our MAM services (MAMfsaHandlerSv, MAMfsaRemoteSV, MAMfsaArchiverSv) run under.)

Finally click **OK**.

🔍 Services							
File Action View	Help						
♦ □ □	Q 🛃 🛛 🖬 🕨 🗖						
🔍 Services (Local)	Name 🔺	Description	Status	Startup Type	Log On As		
	MAM Auditing	Auditing se	Started	Manual	Local System		
	MAM HSM Asynchro	PAM-STOR		Automatic	Local System		
	MAM HSM Base Op	Start	Started	Automatic	Local System		
	Performance Cour	Stop	Started	Mani MAM HSM	Base Operatio	ons Properties (Local Compu	ter) 👂
	Performance Logs	Pause	Started	Mani	Les On Le	1	
	Plug and Play	Resume		Mani General	Log Un Reco	overy Dependencies	
	PnP-X IP Bus Enur	Restart	Started	Mani Logion	as:		
	Portable Device El	All Tacks 🕨 🕨	Started	Mani			
	Print Spooler		Started	Mani C Loc	cal System accou	int	
	Problem Reports a	Refresh	Starteu	Mani 📃	Allow service to i	nteract with desktop	
	Remote Access A	Properties .		Mani 🔎 Thi	a account:	adm@tests.local	Browse
	Remote Access Cr	-	Started	Auto	s account.		Diomsc
	Remote Procedure	Help		Disal Pas	sword:	•••••	
	Extended λ Standard	/	· ·				-
, Opens the properties dia	alog box for the current selec	, tion.		Cor	firm password:		
	,			Help m	e configure user .	account log on options	
				<u>110101111</u>			
				You ca	n enable or disab	ole this service for the hardware pi	rohiles listed below:
				Hard	ware Profile		Service
				Unde	cked Profile		Enabled
				I			
				Trouble	shooting using b	arduara profilea Enable	Disable
				TIOUDR	smooting using n		
						OK Cance	el Apply

b) DCOM Rights has to be reduced in two locations to

AuthenticationLevel="None"

ImpersonationLevel="Anonymous"

and after that the IIS have to be reset.

On the HSM Server follow these steps:

- 1. Open machine.config from:
 - **C**:

\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

In case the 64-bit .NET FrameWork open:

C:

\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.co nfig

2. Locate the entry for "processModel" and add:

comAuthenticationLevel="None" comImpersonationLevel="Anonymous"

The entry then looks as follows:

<processModel autoConfig="true" comAuthenticationLevel="None" comImpersonationLevel="Anonymous" />

- 3. Close the config.
- 4. Now run Component Services (click Start /Settings /Control Panel /Administrative Tools /Component Services).
- 5. In the **Component Services** window expand the **Component Services** tree down to **Component Services \Computers \My Computer** and then right-click **My Computer** to open its **Properties** window.
- 6. Switch over to the Default permissions tab. Check Enable Distributed COM on this computer. Then in the Default Authentication Level dropdown box select None and in the Default Impersonation Level select Anonymous.

Click Apply, then OK.

My Computer Propert	ies		? ×					
Default Protocols General	MSDTC Options	M Security						
Enable Distributed	Enable Distributed COM on this computer							
Enable COM Inter	met Services on this co	mputer						
Default Distributed	COM Communication P	roperties						
The Authentication	Level specifies security	y at the packet le	vel.					
Default Authentic	ation Level:	-						
Indie								
The impersonation who is calling them,	level specifies whether , and whether the appli	applications can cation can do op	determine erations					
using the client's ide	entity.							
	ation Level:	-						
Anonymous	Anonymous							
Security for reference and that the default	ce tracking can be prov t impersonation level is	vided if authentic; not anonymous;	ation is used					
Provide additional security for reference tracking								
	OK	Cancel	Apply					

7. Finally reset IIS.

HSM configured for Windows Server firewall

Active Firewall on the **remote** HSM server can cause issues at file retrieving from the archive. To avoid it, the HSM has to be configured properly.

Here are the steps you have to do on Windows Server 2016 / 2019 /2022 hosting HSM while the Firewall is turned on:

 You need to allow DCOM traffic for COM+ Network Access. Open Start / Programs / Administrative tools / Windows Firewall. In the Windows Firewall under Inbound Rules locate COM+ Network Access and right-click it to open its Properties. On the General tab check Enable and then click OK.



2. Now create a New Inbound Rule. To do so, click the **New Rule** in the right upper corner. The wizard opens. Select **Program** and click **Next**.

🔐 Windows Firewall with Advance	d Security							_	
File Action View Help									
🗢 🔿 🔰 📅 🗟 🔽 🗖									
I Windows Firewall with Advanced S	Inbound Rules						Actions		
Inbound Rules	Name		Group 🔺	Profile	Enabled	Action	Inbound Rules		•
Connection Security Rules	Microsoft Office Outlook			Domain	Yes	Allow	New Rule		
🕀 🌉 Monitoring	BITS Peercaching (Content-In)		BITS Peercaching	Any	No	Allow	Filter by Profile		
	Ment Wizard	-	RITS Peerraching	Δmv	No	Allow	I I The by Folie	X	
									'
									>
	Cor Select the type of firewall rule to c	reate.							
	Cor Steps:								
		v	Vhat type of rule would you like to c	meate?					
	Cor Rule Type								
	Cor Program	_							_
	Cor 🧉 Action	· (•	Program					[DCOM-In]	•
	Cor Profile	~	Rule that controls connections to	or a program					
	Cor Name	0	Port						
	🖉 Cor		Rule that controls connections for	or a TCP or	UDP port.				
	Cor	C	Predefined:						
	Cor		BITS Peercaching				 T		
	Cor		Rule that controls connections for	or a Window	s experience	ə.			
	Cor		Rule that controls connections for	or a vvindow	is experience	ə.			

3. On the next page select **This program path** and browse **<installDir>\Common Files\PAM\HSM\PamHSMTSv**. Click **Next**.



4. Select Allow the connection and click Next. Then click Next again.

5. On the next page name it e.g. **HSM Base Service** and click **Finish**.

🔐 Windows Firewall with Advance	ed Security					
File Action View Help						
🗢 🔿 🖄 🖬 🗟 🖬						
Windows Firewall with Advanced S	Inbound Rules					
Inbound Rules	Name	Group 🔺	Profile	Enabled	Action	
Connection Security Rules	Microsoft Office Outlook		Domain	Yes	Allow	
🕀 🌉 Monitoring	BITS Peercaching (Content-In)	BITS Peercaching	Any	No	Allow	
	New Inbound Rule Wizard		-			
	Specify the name and description o	f this rule.				
	Steps:					
	C a Rule Type					
	Program					
	C Action					
	🖉 Cc 🞍 Profile	Name:				
	Name	HSMI Base Service				
	2 Ca	Description (optional):				

6. Open the **Properties** of the new created Inbound Rule and on the **General** tab click Enable. Then click OK.

🎡 Windows Firewall with Advance	ed Security	
File Action View Help		
🗢 🔿 🖄 🔜 🗟 🗊		
Windows Firewall with Advanced S	Inbound Rules	
Connection Security Rules	Name HSM Base Service Properties HSM Base Service HSM Base Service Users and Computers Protocols and Ports Scope Advanced	Action
Ε 🍢 Monitoring	Mild Barrownice Conde General Programs and Services BITS Peercaching (Con General General	Allow
	Object Bits Peer caching (WSL Object Name: Occord HSM Base Service	Allow
	Core Networking - Des Core Networking - Des Core Networking - Dyn	Allow
	Core Networking - IPvé	Allow
	Core Networking - Mult	Allow
	Core Networking - Neig Core Networking - Neig Core Networking - Pad Core Networking - Pad Block the connections	Allow Allow Allow
	Core Networking - Para Core Networking - Rou Core Networking - Tere Core Networking - Tere	Allow Allow
	Core Networking - Time Core Networking - Router Sc Distributed Transaction OK Cancel Anniu	Allow Allow Allow
	Ork Cancer Poppy Ork Ork Cancer Poppy Ork Cancer Poppy Ork Cancer Poppy	Allow Allow

- Now allow Remote Access and Remote Activation for Everyone in DCOMs. To do so, open Component Services (e.g. unfold the tree down to Component Services \ Computers \ My Computer). Open My Computer Properties. On the COM Security tab:
 - In the Access Permissions section click Edit Limits. In the popup dialog make sure to select Remote Access for Everyone. Finish by clicking OK.

then

• In the Launch and Activation Permission section click Edit Limits. In the pop-up dialog make sure to select Remote Activation for Everyone. Finish by clicking OK.



8. Finally, you can test the connection with HSM tester from the Archive Manager Server.

About Us

6

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.guest.com.

Contacting Quest

For sales or other inquiries, visit <u>www.quest.com/contact</u>.

Technical Support Resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal activates you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product